I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Membership Lists, Metadata, and Freedom of Association's Specificity Requirement

KATHERINE J. STRANDBURG*

Over the past year, documents revealed by leaker Edward Snowden and declassified by the government have provided a detailed look at some aspects of the National Security Agency's (NSA's) surveillance of electronic communications and transactions. Attention has focused on the NSA's mass collection from major telecommunications carriers of so-called "telephony metadata," which includes dialing and dialed numbers, call time, duration, and the like.[1] The goal of comprehensive metadata collection is what I have elsewhere called "relational surveillance"[2]—to follow "chains of communications" between "telephone numbers associated with known or suspected terrorists and other telephone numbers" and then to "analyze those connections in a way that can help identify terrorist

* Alfred B. Engelberg Professor of Law, New York University School of Law. Professor Strandburg acknowledges the generous support of the Filomen D'Agostino and Max E. Greenberg Research Fund.

[1] The term "metadata" has been widely adopted in discussing the NSA's data collection activities and so I will use it here. When one moves beyond call traffic data, however, the term's meaning in the data surveillance context is problematic, ill-defined and may obscure the need for careful analysis. As one illustration of these issues, consider NSA documents recently made public in connection with news reports of NSA monitoring of text messages, which refer, in language that would have made the Red Queen proud, to "content derived metadata." *See* James Ball, *NSA Dishfire Presentation on Text Message Collection—Key Extracts*, THE GUARDIAN, Jan. 16, 2014, *available at* http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents.

[2] Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 1 (2008).

operatives or networks."[3] The program's compliance with statutory authority, its constitutionality under the Fourth and First Amendment, and its counterterrorism value, are now highly contested. This article contends that relational surveillance using so-called metadata implicates the First Amendment right to freedom of association.[4] In particular, it argues that the First Amendment imposes specificity requirements on government acquisition of associational information that are not met by the NSA's comprehensive and undifferentiated collection and scrutiny of associational information.[5]

Today's controversy brings some sense of déjà vu. In December 2005, the *New York Times* created a similar firestorm when it reported that, in the aftermath of the September 11, 2001 terrorist attacks, President Bush had issued executive orders authorizing the NSA to conduct warrantless surveillance of telephone calls and emails from the United States to recipients abroad.[6] In the initial reports, references to the use of "chains of phone numbers and e-mail addresses" to search for "patterns that might point to terrorism suspects" were intermingled with discussion of "warrantless wiretapping" of communication content.[7] Indeed, one unnamed

---

[3] ADMINISTRATION WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 13 (Aug. 9, 2013), *available at* http://op.bna.com/der.nsf/id/sbay-9aeu73/$File/Administration%20White%20Paper%20Section%20215.pdf [hereinafter OBAMA ADMIN. WHITE PAPER].

[4] This article builds on the treatment of this issue in Strandburg, *supra* note 2; *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 147-49 (2007).

[5] *See also*, Solove, *supra* note 4, at 158.

[6] James Risen & Eric Lichtenblau, *Bush Secretly Lifted Some Limits on Spying in U.S. after 9/11, Officials Say*, N.Y. TIMES, Dec. 15, 2005, *available at* http://www.nytimes.com/2005/12/15/politics/15cnd-program.html?pagewanted=all.

[7] *See, e.g., id*; Eric Lichtenblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, *available at* http://www.nytimes.com/2005/12/24/politics/24spy.html?pagewanted=all; Lowell Bergman et al., *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, *available at* http://www.nytimes.com/2006/01/17/politics/17spy.html?ex=1295154000&en=f3247cd88fa84898&ei=5090 ("the agency collected much of the data passed on to the FBI as tips by tracing phone numbers called by suspects overseas, and then by following the domestic numbers to other numbers called"); John Markoff, *Taking Spying to Higher Level, Agencies Look for More Ways to Mine Data*, N.Y. TIMES, Feb. 25, 2006, *available at* http://www.nytimes.com/2006/02/25/technology/25data.html?pagewanted=all (discussing Electronic Frontier Foundation lawsuit against AT&T alleging that "the AT&T

"telecommunications expert" told the *New York Times* in December 2005 that while communications content was "useful," the "real plum" was "the transaction data and the traffic analysis."[8] On May 11, 2006, *USA Today* reported that the NSA had been "secretly collecting the phone call records of tens of millions of Americans" and hoped to "create a database of every call ever made" within the United States in order to "analyze calling patterns in an effort to detect terrorist activity." [9] While that report focused public attention on metadata collection for a time, the metadata issue did not seem to develop independent salience in the debate.

In 2007, Congress passed legislation replacing the Foreign Intelligence Surveillance Act's (FISA's) requirement of individual warrants for surveillance of cross-border communications with a more permissive approach based on programmatic approval of automated monitoring by the Foreign Intelligence Surveillance Court (FISC). Citizens may well have assumed that since bulk metadata collection was not authorized by the 2007 FISA amendments, it would be discontinued. We now know that by 2007 the Bush administration had sought and obtained the FISC's approval for comprehensive collection of communication traffic data under a broad interpretation of pre-existing legal authorities. Between 2004 and 2011, when it discontinued the program, the NSA was authorized by the FISC to collect "internet metadata" under FISA's pen register authority. It obtained FISC approval for its bulk collection of "telephony metadata" under Section 215 of the Patriot Act beginning in 2006.[10] In 2012, Senators Ron Wyden and Mark Udall wrote to the attorney general about the "dangers of relying on secret interpretations of public laws," arguing that "most Americans would be stunned to learn" how Section 215 had been interpreted and that many members of Congress would

---

Daytona system, a giant storehouse of calling records and Internet message routing information, was the foundation of the N.S.A.'s effort to mine telephone records without a warrant").

[8] Lichtenblau & Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, *supra* note 7.

[9] *See, e.g.*, Barton Gellman & Arshad Mohammed, *Data on Phone Calls Monitored Extent of Administration's Domestic Surveillance Decried in Both Parties*, WASH. POST, May 12, 2006, at A1; Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at 1A. This article updates and expands upon my 2008 article responding to those revelations.

[10] *See, e.g.*, Office of the Director of National Intelligence, *DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001*, IC ON THE RECORD (Dec. 21, 2013), *available at* http://icontherecord.tumblr.com/.

be "surprised and angry" to learn of these broad interpretations.[11] The controversy that erupted after Edward Snowden's June 2013 leak of the FISC's order reauthorizing the NSA's bulk telephone metadata collection bears out the senators' predictions.[12]

Writing this article brings some sense of déjà vu as well. I first wrote about freedom of association and relational surveillance in response to the 2006 allegations of bulk collection of telephone traffic data. In some respects, things are different this time around. The legality of the NSA's all-encompassing collection of "metadata" is now front and center in the public debate. Congress has conducted numerous hearings about the program and is considering legislation to contain it to various degrees. President Obama appointed a Review Group on Intelligence and Communications Technologies, which produced a report in December 2013 recommending significant restriction of the program and of related surveillance authorities.[13] The telephone metadata program also has been challenged in court, with two district courts coming to opposite conclusions as to its constitutionality under the Fourth Amendment.[14] Most recently, the independent, bipartisan Privacy and Civil Liberties Oversight Board (PCLOB), established pursuant to the 9/11 Commission Act, issued a scathing condemnation of the metadata program based on its review of publicly available and classified materials.[15] The PCLOB Report was particularly damning in concluding, as have other critics, that the

---

[11] Letter from Sens. Ron Wyden and Mark Udall to Attorney General Eric Holder (Mar. 15, 2012).

[12] *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[13] RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (Dec. 12, 2013) [Hereinafter PRESIDENT'S REVIEW GROUP REPORT].

[14] *Compare* Klayman v. Obama, CV 13-0851 (D.D.C. Dec. 16, 2013) (finding the program likely unconstitutional) *with* ACLU v. Clapper, 13 Civ. 3994 (S.D.N.Y. Dec. 27, 2013) (holding that the program is constitutional).

[15] DAVID MEDINE ET AL., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014) [hereinafter PCLOB REPORT].

program has shown "minimal value in safeguarding the nation from terrorism."[16]

The argument that the mass collection of call traffic data affects freedom of association rights has gained some traction. Notably, the PCLOB devoted a section of its report to the issue, concluding "we can say clearly that the [Section] 215 program implicates First Amendment rights—rights that must be considered in any policy assessment of the program," but stopping short of concluding that the program is unconstitutional under current freedom of association doctrine. For the most part, however, the legal debate remains centered around statutory and Fourth Amendment arguments.

This article makes a renewed pitch for the importance of the First Amendment in assessing the legality of government collection and mining of data that can be, and is intended to be, used to monitor citizens' associations with one another. Part I briefly reviews how metadata collection relates to freedom of association doctrine and concerns and argues that the doctrine must be extended to metadata collection and analysis if freedom of association is to continue to have teeth in the face of technological change. Part II argues that the requisite strict or "exacting" scrutiny of government acquisition of information about individuals' associations imposes three specificity requirements. First, acquisition of *particular* associational information must promote a *specific* compelling government interest. Second, it must have a sufficiently close nexus to that specific interest. Third, the acquisition must be necessary, in the sense that there are no substantially less burdensome means to achieve that specific interest. Because the government often can demonstrate a compelling interest in acquiring at least some associational information, strict scrutiny rarely is the "trump card" it is purported to be in free speech cases. Instead, the action centers around the requirement that government acquisition of associational information be tailored to the government interest. Part III discusses the relationship between these specificity requirements and the "good faith investigation" approach some courts have taken to claims that undercover investigations violate First Amendment freedom of association rights. Part IV describes how the First Amendment's specificity requirements apply to the NSA's "telephony metadata" program as authorized by the FISC since 2004. It then considers the modifications laid out in President Obama's January 17, 2014 speech, as well as the recommendations of the President's Review Group and the PCLOB. Part V concludes.

---

[16] *Id.* at 11.

I. THE DATA MINING RISK TO FREEDOM OF ASSOCIATION

A. *The Freedom to Associate with Others*

The Supreme Court has emphasized that "'implicit in the right to engage in activities protected by the First Amendment' is 'a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends.' This right is crucial in preventing the majority from imposing its views on groups that would rather express other, perhaps unpopular, ideas."[17] Consistent with core First Amendment concerns, freedom of association doctrine protects "expressive association,"[18] in which individuals come together to express themselves "public[ly] or private[ly]."[19] Like protected expression, protected expressive association is broadly defined: "[A]ssociations do not have to associate for the 'purpose' of disseminating a certain message in order to be entitled to the protections of the First Amendment. An association must merely engage in expressive activity that could be impaired in order to be entitled to protection."[20]

Freedom of association was first recognized in cases involving governmental attempts to acquire information about associational affiliations. Thus, in a seminal case, the Court quashed Alabama's request for an NAACP membership list, comparing it to a requirement that members wear identifying armbands:

> This Court has recognized the vital relationship between freedom to associate and privacy in one's

---

[17] Boy Scouts of Am. v. Dale, 530 U.S. 640, 648, 657-58 (2000) (quoting Roberts v. U.S. Jaycees, 468 U.S. 609 (1984) for the proposition that protection of the right to expressive association is "especially important in preserving political and cultural diversity and in shielding dissident expression from suppression by the majority"). Freedom of association protection has particular concern for, but is not limited to, unpopular associations, as is evident from the Court's ruling in *Boy Scouts*, which perhaps could not have involved a more popular organization. *See also, e.g.*, Britt v. Superior Court, 574 P.2d 766 (Cal. 1978).

[18] *Boy Scouts of Am.*, 530 U.S. at 653. Note that the Court also has recognized rights to "intimate association." *Id.* at 646. Though ubiquitous data collection obviously implicates those rights as well, this article focuses on expressive association. The article also assumes, without endorsing, the viability of the distinction between expressive, intimate and "other" association. *Id.*

[19] *Id.* at 650.

[20] *Id.* at 655. *See also, e.g.*, *In re* Motor Fuel Temperature Sales Practices Litigation, 641 F.3d 470, 488 (10th Cir. 2011); *In re* Grand Jury Proceeding, 842 F.2d 1229, 1234 (11th Cir. 1988).

> associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said []: "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[21]

A separate line of cases considers government actions that directly compel, prohibit or otherwise burden the right to associate freely.[22]

Both threads of freedom of association case law apply strict, or "exacting," scrutiny, requiring that government actions that burden freedom of association be "adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms."[23]

Courts have subjected compelled disclosure of associational information to First Amendment scrutiny in cases involving statutes,[24] grand jury and administrative subpoenas,[25] and civil discovery[26] and

---

[21] NAACP v. Alabama, 357 U.S. 449, 462 (1958). *See also* Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963); Bates v. City of Little Rock, 361 U.S. 516 (1960).

[22] *See, e.g.*, *Boy Scouts of Am.*, 530 U.S. at 640; *Roberts*, 468 U.S. 609.

[23] Knox v. SEIU, 132 S. Ct. 2277 (2012) (applying *Roberts* standard); *Boy Scouts of Am.*, 530 U.S. at 659 (applying *Roberts* standard and refusing to apply *O'Brien* intermediate scrutiny standard); *Roberts*, 468 U.S. at 623. *See also* Buckley v. Valeo, 424 U.S. 1, 64 (1976) ("[w]e long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest"); *Gibson*, 372 U.S. at 546 ("regardless of the label applied, be it "nexus," "foundation," or whatever – [] it is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest"); *Bates*, 361 U.S. at 524 (1960); *NAACP v. Alabama*, 357 U.S. at 462–64 (1958) (state must demonstrate interest in obtaining membership lists that is "compelling").

[24] *See, e.g.*, Shelton v. Tucker, 364 U.S. 479 (1960); Paton v. La Prade 469 F. Supp. 773 (D.N.J. 1978).

[25] *See, e.g.*, *Gibson*, 372 U.S. 539; *In re Grand Jury Proceeding*, 842 F.2d 1229 (grand jury subpoena for membership records of tax protest organization); Brock v. Local 375, 860

have deemed the usual relevance standard applied to subpoenas and discovery orders too lax.[27] Courts also have held that disclosure mandates directed to third parties, such as banks, must meet the same strict or exacting standard of scrutiny.[28] In *In re First National Bank*,[29] for example, the Tenth Circuit Court of Appeals distinguished *U.S. v. Miller*, in which the Supreme Court had held that there was no Fourth Amendment expectation of privacy in financial records in third party hands.[30] The First Amendment applied to bank records "because the constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third

---

F.2d 346 (9th Cir. 1988); EEOC v. Univ. of Penn., 850 F.2d 969 (3d Cir. 1988); St. German of Alaska v. United States, 840 F.2d 1087 (2d Cir. 1988); *In re* Grand Jury Proceedings a Grand Jury Witness, 776 F.2d 1099 (2d Cir. 1985); In re Grand Jury Subpoena First Nat. Bank, Englewood, Colo., 701 F.2d 115 (10th Cir. 1983); Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n, 667 F.2d 267 (2d Cir. 1981); United States v. Citizens State Bank, 612 F.2d 1091 (8th Cir. 1980); *In re* Grand Jury Subpoenas to Locals 17, 135, 257, and 608, 528 N.E.2d 1195 (N.Y. 1988) (grand jury subpoena for union membership records).

[26] *See, e.g.*, Perry v. Schwarzenegger, 591 F.3d 1147 (9th Cir. 2010); Snedigar v. Hodderson, 114 Wn.2d 153 (Wash. 1990); New York State Nat'l Org. for Women v. Terry, 886 F.2d 1339 (2d Cir. 1989); Grandbouche v. Clancy, 825 F.2d 1463 (10th Cir. 1987); ETSI Pipeline Project v. Burlington Northern, Inc., 674 F. Supp. 1489 (D.D.C. 1987); Britt v. Superior Ct., 20 Cal. 3d 844 (Cal. 1978).

[27] *See, e.g.*, FEC v. The Larouche Campaign, 817 F.2d 233, 235 (2d Cir. 1987) ("[h]owever, as the court below recognized, different considerations come into play when a case, as here, implicates first amendment concerns. In that circumstance the usual deference to the administration agency is not appropriate, and protection of the constitutional liberties of the target of the subpoena calls for a more exacting scrutiny of the justification offered by the agency"). *See also Perry*, 591 F.3d at 1161 ("[i]mportantly, the party seeking the discovery must show that the information sought is highly relevant to the claims or defenses in the litigation – a more demanding standard of relevance than that under *Federal Rule of Civil Procedure 26(b)(1)*. The request must also be carefully tailored to avoid unnecessary interference with protected activities, and the information must be otherwise unavailable"); *EEOC*, 850 F.2d at 979–80. *But see* Reporters Comm. for Freedom of the Press v. AT&T, 593 F.2d 1030, 1049–50 (D.C. Cir. 1978).

[28] *See, e.g.*, New York Times v. Gonzalez, 459 F.3d 160 (2d Cir. 2006); *Local 1814*, 667 F.2d 267; *In re First Nat. Bank*, 701 F.2d 115; *United States v. Citizens State Bank*, 612 F.2d 1091; Malibu Media v. Does, No. 12-2077, 1–15 (E.D. Pa. 2012); Rich v. City of Jacksonville, Case No. 3:09-cv-454-J-34MCR (M.D. Fla. 2010). *See also Paton*, 469 F. Supp. at 774-82 (regulation allowing government to request postal service to conduct "mail cover" when necessary "to protect the national security" complied with the Fourth Amendment, but ran afoul of the First Amendment's protection of freedom of association).

[29] 701 F.2d at 117–18.

[30] *Id.* (discussing U.S. v. Miller, 425 U.S. 435, 444 (1976)).

parties."[31] This distinction between First and Fourth Amendment applicability is directly relevant to metadata surveillance, which involves data collected from third party service providers.

B. *Association in a Digitally Networked Era*

Technological and societal developments have led to an ever-increasing role for digitally intermediated social interactions. The speed and asynchronous nature of Internet communication, along with the high connectivity and information advantages of social networks, lower the costs of collective activity and decrease the importance of geographical proximity, thereby empowering individuals to associate with one another in expressive activities of all kinds.[32] These developments are useful for traditional membership organizations. Perhaps even more importantly, they enable emergent and dynamic forms of expressive association that may or may not coalesce into traditional organizational form. These same techno-social developments mean that individuals leave ever more detailed and comprehensive trails of data reflecting their activities. That data, like the GPS location data at issue in the recent Fourth Amendment case, *United States v. Jones*, "generates a precise, comprehensive record . . . that reflects a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations."[33]

In addition to these trends, which I discussed in my 2008 article, the availability of so much data about individuals now drives a tendency to see "big data" analysis as a panacea approach to solving

---

[31] *Id.* at 118. *See also New York Times*, 459 F.3d at 163 ("whatever rights a newspaper or reporter has to refuse disclosure in response to a subpoena extends to the newspaper's or reporter's telephone records in the possession of a third party provider"); *In re Grand Jury Proceeding*, 842 F.2d at 1233 (rejecting argument that the first amendment affords no "extra margin of privacy" by imposing substantive or procedural restrictions on good faith criminal investigations beyond the limits imposed by the Fourth and Fifth Amendments); *Reporters Comm. for Freedom of the Press*, 593 F.2d at 1071 n. 4 (Robinson, J., concurring) ("the analysis appropriate for First Amendment issues concentrates on the burden inflicted on protected activities, and the result may not always coincide with that attained by application of Fourth Amendment doctrine"). *Cf. Reporters Comm. for Freedom of the Press*, 593 F.2d at 1054 ("[i]n my view, the guarantees of the Fourth and Fifth Amendments achieve their purpose and provide every individual with sufficient protection against good faith investigative action for the full enjoyment of his First Amendment rights of expression") (portion of majority opinion joined only by its author, Wilkey, J.).

[32] See the discussion in Strandburg, *supra* note 2, at 745–46.

[33] United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

society's problems.[34] Strong, and sometimes extravagant, claims about big data's revolutionary potential increasingly are common. Entire industries have come to depend on big data's promise. Big data optimism fuels attempts by everyone from industry to researchers to governments to create, acquire, and store more and more data. For those caught up in the big data enthusiasm, it becomes easy to assume that the answer to questions about the effectiveness and usefulness of data mining is simply more data.

C. *How Data Mining Potentially Undercuts Traditional Doctrine*

Traditional freedom of association doctrine is rooted in an era in which the danger of unwarranted government intrusion into individuals' freedom to associate lay primarily in the government's ability to monitor the activities of centrally organized groups with names, platforms, membership lists, and the like. The doctrine thus assumes a process in which the government first identifies an organization that it deems suspicious or threatening and then attempts to obtain a list of the organization's members or affiliates by demanding it from the organization or from a third party. If such a demand is challenged, the analysis begins by determining whether the organization is an "expressive association," then proceeds, at least in some courts, to assess whether there is a "prima facie case" that the demand would burden the freedom of association of its members. Only then does the court conduct the First Amendment inquiry into whether the government has a compelling interest in acquiring the information and whether that interest could be "achieved through means significantly less restrictive of associational freedoms."[35]

Data mining takes the teeth out of this traditional approach. Data can be collected indiscriminately and mined later. Without focusing on any "expressive association" at the time of collection, the government can acquire and aggregate information about individuals' transactions, communications, locations and the like. That information can be used to infer many, if not most, of the citizenry's associational activities. Thus, such associational data can be used to make precisely the kind of government inquiry that freedom of association doctrine evolved to curtail. It also can be used, even more intrusively, to expose informal, exploratory and tentative associations for which no formal membership lists exists.

---

[34] *See, e.g.*, Gil Press, *A Very Short History of Big Data*, FORBES, May 9, 2013, *available at* http://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/.

[35] *Boy Scouts of Am.*, 530 U.S. at 680 (citing *Roberts*, 468 U.S. 609).

Moreover, data mining is an exercise in inference based on models and assumptions about the social meaning of the data. (For example, a data mining investigation of association based on call traffic data might assume that the frequency of calls is a proxy for "closeness" in some social sense.) Data mining thus can simultaneously be extraordinarily intrusive and prone to error.[36] Moreover, while joining or making financial contributions to a controversial organization is a deliberate act, individuals are not privy to the models and assumptions governments employ in analyzing associational data. They thus are left to guess about which of their activities might lead a data mining algorithm to "predict" that they are affiliated with a disfavored, criminal, or terrorist group. Under these circumstances, citizens' awareness that "the Government may be watching" their patterns of communication and other associational data has particularly great potential to "chill . . . associational and expressive freedoms."[37]

Government collection and mining of associational data thus may chill a broader swath of associational activities than compelled disclosure of membership in controversial organizations. It may deter individuals from associating even informally or temporarily to explore and express controversial views. Its potential for erroneous inference further encourages individuals to steer well clear of anyone they (rightly or wrongly) fear might be engaging in controversial activities. Moreover, because data mining is probabilistic, the social meaning of an association inferred from data mining often will be unclear. Government agents will need to investigate further to determine whether "suspicious" associations uncovered by the analysis are problematic or benign. The burden of these investigations is likely to extend beyond those who have chosen to engage in controversial activities and to weigh particularly heavily on members of some ethnic, religious, or political communities. Such investigations are likely to chill the associational activities of members of such communities over and above the chilling effect produced by knowing about government data collection and mining.

A common response to these concerns is that the government's purpose for collecting associational data is only to uncover information about criminal or terrorist associations and that those who have "nothing to hide" have nothing to fear. This response is inadequate for several important reasons. Most obviously, the lessons of history repeatedly tell us that the power to investigate individuals'

---

[36] *See* Strandburg, *supra* note 2, for further discussion of this point.

[37] *Jones*, 132 S. Ct. at 956.

associations is subject to abuse, not only by rogue government officials, but also by government officials who are overzealous in their law enforcement or security missions and do not give adequate weight to other important values. Indeed, if that were not the case, there would be little need for the First Amendment's freedom of association protections.

Equally important, democratic majorities cannot be counted upon to protect the interests of religious, ethnic, political, and other minorities in balancing security and liberty. This core First Amendment concern underlies many of the early freedom of association cases, which involved demands for membership lists from the NAACP and Communist Party during the 1950s and 60s. It is easy to take a hindsight view of these actions, attributing them to irrational animus that is no longer a motivating factor in today's law enforcement and counterterrorism efforts. While there undoubtedly is truth to this view, we should recall that these democratically-blessed intrusions were justified at the time by the fear and belief that these organizations harbored individuals with violent designs. One of the First Amendment's important purposes is to protect democratic values from present-day myopia.

We thus stand at a crossroads for freedom of association. If we do not extend its protections to government collection and mining of associational data we may soon find that freedom of association has become an empty shell.

D. *Constitutional Interpretation in Light of Techno Change*

The question of how constitutional rights should be interpreted in light of technological change is a large one that is mostly beyond the scope of the present article. To move forward though, some principles are useful. In my 2008 article, I relied on the ways in which the Supreme Court has confronted technological change in the Fourth Amendment context to suggest three lessons for assessing the First Amendment's implications for relational surveillance.[38] Restating and slightly generalizing, those lessons were: 1) That constitutional interpretation should account for the ways in which social behavior responds to new technology; 2) that new technologies for analyzing data can change the constitutional balance; and 3) that constitutional assessment should be sensitive to the extent to which particular surveillance techniques intrude upon legitimate, as well as illicit, behavior. Here I argue that these lessons derive from an additional,

---

[38] Strandburg, *supra* note 2.

and more fundamental, principle, which is that technological advancement cannot be allowed to vitiate constitutional protections.

The first lesson relates primarily to technology that is used by the public. In 1967, *Katz v. United States*,[39] overruled *Olmstead v. United States*,[40] decided in 1928, to hold that wiretapping a phone line was a Fourth Amendment search requiring a warrant. *Katz* and *Olmstead* took dramatically different views of the role of the telephone in social life. *Olmstead* viewed the telephone as a means by which the caller "projects his voice to those quite outside" of his home and analogized the telephone wires to "the highways along which they are stretched."[41] *Katz* ruled that the Fourth Amendment's protection extended to telephone calls because "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in *private* communication."[42] *Katz* thus recognized that the invention of the telephone and its incorporation into social life had fundamentally changed the way in which private relationships were conducted; failure to recognize that intertwined techno-social change would have reduced Fourth Amendment protections dramatically.

The second and third lessons relate to surveillance technology. In 2001, *Kyllo v. United States*[43] held that using thermal imaging to "see" inside a house was a search regulated by the Fourth Amendment. The thermal imaging technology did no more than measure infrared radiation that was emitted into the "plain view" of passersby and analyze the data. Yet the Court specifically rejected the dissent's argument that such use of technology to make inferences from publicly available data could not constitute a search.[44] The majority recognized that "[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy" and held that the use of thermal imaging was a Fourth Amendment-regulated search.[45] The Court thus recognized, at least implicitly, that rigid adherence to doctrinal formulations developed in

---

[39] 389 U.S. 347 (1967). *Katz* is famous for its statement that "the Fourth Amendment protects people, not places" and for Justice Harlan's concurrence, in which he proposed the "reasonable expectation of privacy" test.

[40] 277 U.S. 438 (1928).

[41] *Id.* at 465-66.

[42] *Katz*, 389 U.S. at 512. (Emphasis added.)

[43] 533 U.S. 27 (2001).

[44] *Id.* at 35-36. *See also id.* at 42-44 (Stevens, J. dissenting).

[45] *Id.* at 34.

an earlier technological milieu is not appropriate when those formulations no longer reflect technological realities.

In 2005, the Court held that a "dog sniff" for narcotics did not constitute a Fourth Amendment search despite the similar use of technology (the dog) to make inferences from publicly detectable emanations.[46] The Court distinguished *Kyllo* because the "dog sniff" revealed only illegal activity (or so the Court assumed), noting that "[c]ritical to [the *Kyllo*] decision was the fact that the device was capable of detecting lawful activity."[47] A more subtle question arose in *Florida v. Harris*,[48] decided in 2013. There the Court considered whether a drug dog's "alert" was enough to constitute probable cause for a search of a truck.[49] The controversy revolved around whether the dog's drug detection skills were accurate enough to establish probable cause. Though overturning the lower court's ruling that there was insufficient evidence of the dog's accuracy, the Court did not question the defendant's right to challenge the accuracy of the dog sniff "technology." Taken together with Kyllo, these cases reveal that the accuracy with which a surveillance technology discriminates between legitimate and illicit activity is of constitutional significance. Government assertions about the efficacy of particular investigative techniques need not be taken at face value, but may be challenged.

Undergirding these specific lessons is the more general principle that technology, whether employed by the public or by government officials, cannot be allowed to vitiate constitutional rights. The next Part of this article argues that freedom of association imposes specificity requirements that are crucial to maintaining the viability of First Amendment freedom of association protection in an era of ubiquitous data trails.

II. FREEDOM OF ASSOCIATION'S SPECIFICITY REQUIREMENT

A. *The Chilling Effects of Sweeping Acquisition of Associational Information*

Like the right to free speech, freedom of association is concerned with avoiding governmental action that suppresses particular

---

[46] Illinois v. Caballes, 543 U.S. 405 (2005).

[47] *Id.* at 409.

[48] 133 S. Ct. 1050, 1053 (2013).

[49] *Id.*

expressive purposes, views, and activities unless there is a compelling reason to do so. There are a number of mechanisms by which government acquisition of associational information might produce "chilling effects" that would suppress particular sorts of expressive association. Chilling effects arise when individuals are concerned that disclosing particular associational activities to the government or to the public at large will subject them to harassment or other adverse effects.

If governments are free to demand that unpopular groups turn over their membership lists and other associational information and to use that information as they please, it is likely that citizens will be deterred from joining such groups. While cases involving laws that explicitly compel disclosure by particular groups are rare,[50] a number of cases, including *NAACP v. Alabama*, involve demands targeted at particular groups under cover of generally applicable regulations.[51] While it might seem that broad-based collection of associational information would pose less risk of chilling effects, the Court's opinion in *Shelton v. Tucker*[52] explains why sweeping collection can be no less chilling.

In *Shelton*, a state statute required that teachers annually disclose to the state all organizations to which they had belonged within the preceding five years. Though *Shelton* had factual roots in hostility toward the NAACP,[53] the Court's analysis did not rely on those roots. Instead, the Court's analysis turned on the breadth of disclosure compelled by the statute. The Court observed that while "there can be no question of the relevance of a State's inquiry into the fitness and competence of its teachers, "it is not disputed that to compel a teacher to disclose his every associational tie is to impair that teacher's right of free association . . . which, like free speech, lies at the foundation of a free society."[54] The impairment of the teachers' rights to associate freely resulted from the breadth of the required disclosure, rather from a showing that any particular group would be adversely affected:

---

[50] *See, e.g.*, Communist Party v. Subversive Activities Control Bd., 367 U.S. 1 (1961).

[51] 357 U.S. at 451.

[52] 364 U.S. 479 (1960).

[53] The lower court also had invalidated a state statute making state employment of NAACP members unlawful. *Id.* at n. 2 (citing Shelton v. McKinley, 174 F. Supp. 351 (E.D. Ark. 1959)).

[54] *Shelton*, 364 U.S. at 485-86.

> The scope of the inquiry required by Act 10 is completely unlimited. The statute requires a teacher to reveal the church to which he belongs, or to which he has given financial support. It requires him to disclose his political party, and every political organization to which he may have contributed over a five-year period. It requires him to list, without number, every conceivable kind of associational tie-social, professional, political, avocational, or religious.[55]

Far from mitigating the chilling effects, the "unlimited and indiscriminate sweep" of the collection, along with the government's discretion in making use of the information, left teachers uncertain as to which of their associations might be displeasing to someone in a position of power, with the result that "the pressure upon a teacher to avoid any ties which might displease those who control his professional life would be constant and heavy."[56]

Other cases similarly strike down demands for membership information that are "sweeping and indiscriminate." In *In re Stolar*, for example, the Court struck down a state bar committee's demand that applicants list all of their association memberships,[57] despite the legitimate state interest in investigating character and competence to practice law. The Court emphasized the burden imposed by the breadth of the inquiry: "[T]he listing of an organization considered by committee members to be controversial or "subversive" is likely to cause delay and extensive interrogation or simply denial of admission to the Bar . . . . Law students who know they must survive this screening process before practicing their profession are encouraged to protect their future by shunning unpopular or controversial organizations."[58]

---

[55] *Id.* at 488.

[56] *Id.* at 486.

[57] 401 U.S. 23 (1971). *See also* Baird v. State Bar Ass'n of Arizona, 401 U.S. 1, 6 (1971) ("[b]road and sweeping state inquiries into [associations] discourage citizens from exercising rights protected by the Constitution"); Clark v. Library of Congress, 750 F.2d 89, 104 (D.C. Cir. 1984) ("broad and sweeping inquiry into [plaintiff's] political beliefs and associations" must be "justified by a showing that the investigation was necessary to serve a vital governmental interest" and used the "means least restrictive" of first amendment rights); *Britt*, 574 P.2d at 766 ("[i]n view of the sweeping scope of the discovery order at issue, we think it clear that such order is likely to pose a substantial restraint upon the exercise of First Amendment rights").

[58] *In re Stolar*, 401 U.S. at 28.

When the government acquires information about unpopular, controversial or potentially embarrassing associational activities, the unavoidable effect is to discourage such associations because of the fear that government agents will use the information to impose burdens on those involved. The more sweeping the collection, the greater the fear that it will sweep in information about some associational activity that arouses animus in some government official. The likelihood of a significant chilling effect presumptively grows with the scope of the government's acquisition of associational information. Thus, the Court recognizes that broad government acquisition of associational information is itself evidence that chilling effects are likely.

B. *Freedom of Association's Strict Scrutiny Standard*

As discussed in Part I, freedom of association claims are assessed using strict or "exacting" scrutiny—government actions that implicate freedom of association must be "adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms."[59] In the free speech context, strict scrutiny traditionally has been viewed as a kind of trump card.[60] As courts found it

---

[59] *Roberts*, 468 U.S. at 623; *Boy Scouts of Am.*, 530 U.S. at 640 (applying *Roberts* standard and refusing to apply *O'Brien* intermediate scrutiny standard); *Knox v. SEIU*, 132 S. Ct. 2277 (applying *Roberts* standard). *See also NAACP v. Alabama*, 357 U.S. at 462 (1958) (state must demonstrate interest in obtaining membership lists that is "compelling"). *See also, e.g.*, *Bates*, 361 U.S. at 516; *Gibson*, 372 U.S. at 539 ("regardless of the label applied, be it "nexus," "foundation," or whatever – [] it is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition that the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest."); *Buckley*, 424 U.S. at 64 ("[w]e long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest").

[60] *See, e.g.*, Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VAND. L. REV. 793, 807-08 (2006) (describing this "myth" and quoting Laurence Tribe as saying "there are very few cases which strictly scrutinize and yet uphold instances of impaired fundamental rights"). The idea that strict scrutiny always deals a fatal blow has been undercut in recent years, in part by empirical study demonstrating that regulations do, in fact, survive it. *Id.* Winkler's study showed that religious liberty regulations were most likely to survive strict scrutiny. Tantalizingly, Winkler's results show freedom of association cases as next most likely to survive strict scrutiny, with free speech cases least likely to survive it. Unfortunately, the differences are not statistically significant so one can only speculate that they would hold up with a larger sample size.

necessary or desirable to take conflicting values into account, they developed alternative, "intermediate" levels of scrutiny.[61] Thus, for example, in the free speech context, content-neutral "time, place, or manner regulations"[62] and conduct regulations with incidental effects on speech are subject to intermediate scrutiny.[63]

Freedom of association doctrine generally has not accommodated competing values by introducing varying levels of scrutiny.[64] Strict scrutiny is hardly a trump card in freedom of association cases, however, perhaps because courts take the potential for harm from associational activities more seriously than the potential for harm

---

[61] *See, e.g.*, Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267 (discussing the impact of various intermediate scrutiny tests on the role of strict scrutiny).

[62] Ward v. Rock Against Racism, 491 U.S. 781 (1989).

[63] United States v. O'Brien, 391 U.S. 367 (1968).

[64] The only exceptions are in the electoral context. The Supreme Court has taken a relatively permissive view, for example, of regulations directly affecting who can vote in primary elections. Clingman v. Beaver, 544 U.S. 581 (2005) ("[w]hen a state electoral provision places no heavy burden on associational rights, a State's important regulatory interests will usually be enough to justify reasonable, nondiscriminatory restrictions"). Even in the election context, cases involving compelled disclosure of associational information have maintained a strict or "exacting" scrutiny rubric and for the most part have used those terms interchangeably. *See, e.g.*, *Buckley*, 424 U.S. at 45, 64, 75 ("the constitutionality of [an expenditure limitation] turns on whether the governmental interests advanced in its support satisfy the exacting scrutiny applicable to limitations on core First Amendment rights of political expression." "We long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes cannot be justified by a mere showing of some legitimate governmental interest. Since *NAACP v. Alabama* we have required that the subordinating interests of the State must survive exacting scrutiny." "In considering this provision we must apply the same strict standard of scrutiny, for the right of associational privacy developed in *NAACP v. Alabama* derives from the rights of the organization's members to advocate their personal points of view in the most effective way"). Recently, the Court applied a somewhat less rigorous "exacting scrutiny" in a situation where disclosure of the names of referendum signers was important to the integrity of the electoral process. Doe v. Reed, 130 S. Ct. 2811 (2010). *See id.* at 2822 (Breyer, J., concurring) ("where a law significantly implicates competing constitutionally protected interests in complex ways, the Court balances interests"); *id.* at 2828 (Sotomayor, J., concurring) ("[p]ublic disclosure of the identity of petition signers, which is the rule in the overwhelming majority of States that use initiatives and referenda, advances States' vital interests in preserving the integrity of the electoral process, preventing corruption, and sustaining the active, alert responsibility of the individual citizen in a democracy for the wise conduct of government"). *But see id.* at 2839 (Thomas, J., dissenting) ("I read our precedents to require application of strict scrutiny to laws that compel disclosure of protected First Amendment association"). *Cf.* McIntyre v. Ohio Election Comm., 514 U.S. 334 (1995) (striking down regulation forbidding anonymous campaign pamphlets under strict scrutiny). Outside of the election context, however, strict (or an essentially equivalent exacting) scrutiny is the rule.

from speech.[65] In many cases the government can point to some interest that is compelling at some level of abstraction. For this reason, freedom of association analysis focuses on the nexus between the specific information requested and that interest.

C. *First Amendment Scrutiny as a Specificity Requirement*

First Amendment scrutiny effectively imposes specificity requirements on government acquisition of associational information: Acquisition must promote a specific compelling government interest; the information acquired must have a sufficiently close nexus to that interest; and acquisition must be necessary, in the sense that there are no substantially less burdensome means to achieve that interest.

In *NAACP v. Alabama*, for example, the state sought the identities of the NAACP's members as part of a suit to enforce the state's foreign corporation registration statute. The applicability of the requirement turned on whether the NAACP was conducting intrastate business within the meaning of the statute. The Court did not question the state's interest in enforcing the statute and found no constitutional infirmity in some of the state's requests, for example for the names of directors and officers, the number of members, and the amount of dues collected. The particular request for the names of the organization's rank-and-file members was not permissible, however, because it had no substantial bearing on the applicability of the registration requirement and thus did not further the state's interest in enforcing it.[66]

---

[65] There is, of course, room for debate about the potential for harm from speech. For example, there is a long-running debate about government regulation of hate speech. *See, e.g.*, Jeremy Waldron, *The Visibility of Hate*, 123 HARV. L. REV. 1596 (2010); Richard Delgado & David H. Yun, *Pressure Valves and Bloodied Chickens: An Analysis of Paternalistic Objections to Hate Speech Regulation*, 82 CALIF. L. REV. 871 (1994); Richard Delgado & David H. Yun, *The Neoconservative Case Against Hate-Speech Regulation-Lively, D'Souza, Gates, Carter, and the Toughlove Crowd*, 47 VAND. L. REV. 1807 (1994); Charles R. Calleros, *Paternalism, Counterspeech and Hate Speech Codes: A Reply to Delgado and Yun*, 27 ARIZ. ST. L.J. 1249 (1995); Richard Delgado & David Yun, *First Amendment Totalism, the ACLU, and the Principle of Dialogic Politics*, 27 ARIZ. ST. L.J. 1281 (1995). Some argue that the potential for harm from hate speech on the Internet is particularly great. *See, e.g.*, Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

[66] *See also Bates*, 361 U.S. at 524-25 (while "no power is more basic to the ultimate purpose and function of government than is the power to tax" and a municipal ordinance was enacted as an "adjunct" of that power, the court found "no relevant correlation between the power of the municipalities to impose occupational license taxes and the compulsory disclosure and publication of the membership lists of [the NAACP]").

In *Shelton*, the Court distinguished *NAACP v. Alabama*, where "there was no substantially relevant correlation between the governmental interest asserted and the State's effort to compel disclosure of the membership lists involved," acknowledging that "there can be no question of the relevance of a State's inquiry into the fitness and competence of its teachers."[67] The problem with the state's demand for information was its lack of specificity:

> The question to be decided here is not whether the State of Arkansas can ask certain of its teachers about all their organizational relationships. It is not whether the State can ask all of its teachers about certain of their associational ties. It is not whether teachers can be asked how many organizations they belong to, or how much time they spend in organizational activity. The question is whether the State can ask every one of its teachers to disclose every single organization with which he has been associated over a five-year period.[68]

While some of the requested information might have been relevant to teacher fitness, the state's demand for information had to be judged in light of "less drastic means for achieving the same basic purpose."[69]

In *Buckley v. Valeo*,[70] on the other hand, the Supreme Court upheld a provision mandating disclosure of political contributions against a facial challenge. The Court declined to employ intermediate scrutiny, opining that "the strict test established by *NAACP v. Alabama* is necessary because compelled disclosure has the potential for substantially infringing the exercise of First Amendment rights."[71] The mandate survived because of its important role in: 1) Providing the electorate with information to aid them in evaluating candidates; 2) deterring corruption and avoiding the appearance of corruption; and 3) gathering data needed to detect violations of the statute's contribution limitations. Though disclosure placed "not insignificant burdens on individual rights," it appeared to be the "least restrictive means of curbing the evils of campaign ignorance and corruption that

---

[67] *Shelton*, 364 U.S. at n. 5.

[68] *Id.* at 487-88.

[69] *Id.* at 488.

[70] *Buckley*, 424 U.S. at 1.

[71] *Id.* at 66.

Congress found to exist," particularly since the door remained open for challenges in particular cases.[72] A few years later the Court voided a similar mandate as applied to the Socialist Workers Party (SWP) because the fit between means and ends was insufficient in light of "substantial evidence of past and present hostility from private persons and Government officials" toward the SWP, coupled with the diminished government interests in financial contributions to a minor party.[73]

The government cannot demand a list of members of a legitimate group simply to investigate whether the group has been infiltrated by actors devoted to violent or illegal ends. A tighter nexus is required. Thus, in *Gibson v. Florida Legislative Investigation Committee*,[74] a legislative committee sought a list of NAACP members, purportedly to investigate whether the NAACP had been infiltrated by members of the Communist Party. Though Communist Party membership was "itself a permissible subject of regulation and legislative scrutiny" due to the "particular nature" of that party, "[v]alidation of the broad subject matter under investigation does not necessarily carry with it automatic and wholesale validation of all individual questions, subpoenas, and documentary demands."[75] The demand for the membership list of a "concededly legitimate and nonsubversive organization" ran afoul of the nexus requirement.[76]

In upholding a statute requiring "Communist-action organizations" to disclose membership information, the Court found the necessary nexus in the statute's definition of "communist-action organization" as a group "directed, dominated, or controlled" by and operating "primarily to advance the objectives" of a foreign communist government and in the fact that the designation was made via administrative hearing and subject to judicial review.[77]

A disclosure mandate need not sweep as broadly as the *Shelton* provision to be insufficiently specific in relation to the government's need for associational information. In a civil suit brought against airport authorities by a group of local residents, for example, the California Supreme Court quashed a discovery request for all

---

[72] *Id.* at 68.

[73] Brown v. Socialist Workers '74 Campaign Committee, 459 U.S. 87, 102 (1982).

[74] 372 U.S. at 539.

[75] *Id.* at 545.

[76] *Id.* at 548.

[77] *Communist Party v. Subversive Activities Control Bd.*, 367 U.S. at 7.

documents reflecting the plaintiffs' communications with several organizations engaged in advocacy relating to noise and other issues concerning the airport. The court opined that "[t]he very breadth of the required disclosure establishes that the trial court in this case did not apply traditional First Amendment analysis in passing on the validity of defendant's inquiries into the private associational realm, and in particular did not heed the constitutional mandate that precision of disclosure is required so that the exercise of our most precious freedoms will not be unduly curtailed."[78]

Freedom of association's specificity requirements also are evident in cases in which courts tailor disclosure mandates to the government interest, rather than allowing or denying them wholesale.[79] For example, in a case alleging that longshoremen had been coerced into authorizing payroll deductions for contributions to a union-related political advocacy organization, the court limited a subpoena for members' names to a random ten percent sample of those who had signed up relatively late for the deduction, under the rationale that they were most likely to have been coerced.[80] The limitations were fashioned to ensure that disclosure would "impact a group properly limited in number in light of the governmental objective to be achieved."[81] Courts have also taken steps such as in camera review of evidence and requiring the names of donors be replaced by numbers to protect their identities.[82]

These and other cases demonstrate that specificity requirements stemming from the First Amendment guarantee of freedom of

---

[78] *Britt*, 574 P.2d at 861.

[79] *See, e.g.*, In the Matter of Full Gospel Tabernacle v. New York, 536 N.Y.S.2d 201 (App. Div. 1988); *In re Grand Jury Subpoena for Locals 17, 135, 257, and 608*, 528 N.E.2d 1195; Doyle v. NYS Div. Housing, 715 N.Y.S.2d 52 (S.D.N.Y 2000); Nat'l Org. for Marriage v. Maine Comm'n Governmental Ethics, 66 A.3d 570 (Me. 2013); St. German of Alaska E. Orthodox Catholic Church v. United States, 840 F.2d 1087 (2d Cir. 1992). *But see* Friends Social Club v. Sec'y of Labor, 763 F. Supp. 1386 (E.D. Mich. 1991).

[80] *Local 1814*, 667 F. 2d 267.

[81] *Id.* at 273. *See also, e.g.*, *U.S. v. Citizens State Bank*, 612 F.2d 1091 (suggesting a graduated series of disclosures of associational information); Socialist Workers Party v. Attorney Gen., 642 F.Supp 1357 (S.D.N.Y 1986) (overturning preliminary injunction on undercover investigation, but retaining injunction against sending members' names to Civil Service Commission); *FEC v. Larouche Campaign*, 817 F.2d 233 (FEC justified in obtaining names of contributors, but not in obtaining the names of those who solicited contributions).

[82] *In re* Deliverance Christian Church, No. 11-62306, 2011 WL 6019359 (Bankr. N.D. Ohio Dec. 1, 2011).

association limit the amount of associational information that government may demand. Governments may acquire associational information only when there is a close nexus between the accomplishment of a specific compelling government interest and the particular information to be acquired, as well as a lack of substantially less intrusive means to accomplish the government's purpose. Like the particularity requirements associated with the Fourth Amendment, these specificity requirements should play an important and direct role in regulating government surveillance of expressive association.

III. FREEDOM OF ASSOCIATION SPECIFICITY AND "GOOD FAITH INVESTIGATION"

In defending the NSA's telephony metadata surveillance, the Obama administration has argued that "otherwise lawful investigative activities conducted in good faith—that is, not for the purpose of deterring or penalizing activity protected by the First Amendment—do not violate the First Amendment."[83] In other words, the administration argues that there need be no independent First Amendment scrutiny of law enforcement acquisition of associational information as long as the investigation is not conducted for the *purpose* of chilling protected associational activity.

This argument rests on a misreading of relevant precedent, and is inconsistent with ensuring that governmental acquisition of associational information meets First Amendment standards. The government's compliance with the right to freedom of association is not determined by good intentions,[84] but by whether any chilling effects associated with its acquisition of associational information are justified by a sufficient nexus to a compelling government interest. As the Court explained in *Buckley*, strict scrutiny "is necessary even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct in requiring disclosure."[85]

The good faith investigation standard referenced in the *White Paper* arises out of two lines of case—one dealing with reporter's privileges and the other dealing with undercover investigations. The

---

[83] OBAMA ADMIN. WHITE PAPER, *supra* note 3, at 22.

[84] *See, e.g.*, *Clark v. Library of Congress*, 750 F.2d 89 ("cannot be the sole test of legitimacy").

[85] *Buckley*, 424 U.S. at 65.

Obama Administration White Paper relied heavily on *Reporters Committee for Freedom of the Press v. AT&T*, which dealt with grand jury subpoenas for journalists' phone records. There, the D.C. Circuit Court of Appeals interpreted *Branzburg v. Hayes*, in which the Supreme Court had upheld subpoenas compelling journalists to testify about articles they had published based on confidential sources.[86]

As the Court explained in *Branzburg*:

> The sole issue before us is the obligation of reporters to respond to grand jury subpoenas as other citizens do and to answer questions relevant to an investigation into the commission of crime. . . . The claim is [] that reporters are exempt from these obligations because if forced to respond to subpoenas and identify their sources or disclose other confidences, their informants will refuse or be reluctant to furnish newsworthy information in the future. This asserted burden on news gathering is said to make compelled testimony from newsmen constitutionally suspect and to require a privileged position for them.[87]

The Court refused to confer a special privilege against grand jury subpoenas on journalists, pointing out that grand juries remain "subject to judicial control and subpoenas to motions to quash" if appropriate in particular cases.[88] Justice Powell's concurrence further emphasized that motions to quash on a "case-by-case basis" could strike the "proper balance between freedom of the press and the obligation of all citizens to give relevant testimony with respect to criminal conduct."[89] In any event, the Court opined that the subpoenas at issue in *Branzburg* met the freedom of association standards set out in its membership list disclosure cases. The Court also observed that "grand jury investigation, if instituted or conducted other than in good faith, would pose wholly different issues for resolution under the First Amendment."[90]

---

[86] 408 U.S. 665 (1972).

[87] *Id.* at 682.

[88] *Id.* at 708.

[89] *Id.* at 710.

[90] *Id.* at 707 (emphasis omitted).

In *Reporters Committee for Freedom of the Press v. AT&T*,[91] a group of journalists challenged the use of grand jury and administrative subpoenas to acquire their calling records from their carriers, seeking notice and an opportunity for judicial review before such records were disclosed.[92] The majority interpreted *Branzburg* to hold that "there is no case-by-case consideration given to a claim of privilege," and concluded that journalists do not have a "special right to resist good faith subpoenas directed at a third-party's business records."[93] As a dissent was quick to point out, however, *Branzburg* "turned explicitly on the determination that the prior judicial scrutiny on a case-by-case basis which was afforded [by a motion to quash] was sufficient to protect the First Amendment rights at stake."[94]

The *Reporters Committee* reading of *Branzburg* thus confused the question of a special reporter's privilege with the issue of the First Amendment's requirements in particular cases and, not surprisingly, has been rejected by many other courts.[95] The Second Circuit, for example, explicitly rejected it, holding that subpoenas for reporters' phone records are subject to First Amendment balancing.[96] Consistent with freedom of association's specificity requirement, the Second Circuit suggested that a request for "disclosure of all phone records over a period of time" might be overbroad as yielding "information that bears only a remote and tenuous relationship to the investigation," and that such overbreadth might be cured by redaction of unrelated records.[97] Most importantly for present purposes, *Branzburg* and *Reporters Committee* did not involve government demands for association membership information, but focused on

---

[91] 593 F.2d 1030 (1978).

[92] *Id.* at 1030.

[93] *Id.* at 1049-50.

[94] *Id.* at 1080.

[95] *See, e.g.*, *New York Times*, 459 F.3d at 160; *Local 1814*, 667 F.2d 267; *In re* Grand Jury Subpoena, Judith Miller, 397 F.3d 964, 976 (D.C. Cir. 2005) (concurrence); *In re Grand Jury Proceeding*, 842 F.2d 1229; *In re First Nat'l Bank*, 701 F.2d 115; *Paton*, 469 F. Supp. at 773 ; United States v. Markiewicz, 732 F. Supp. 316 (N.D.N.Y. 1990); *see also* United Transp. Union v. Springfield, No. 87-0342-P, 1989 U.S. Dist. LEXIS 2698 (D. Me. 1989) (declining to follow in civil context); Philip Morris v. American Broad. Co., 36 Va. Cir. 1 (Va. Cir. Ct. 1994) (same); *see also* Parson v. Watson, 778 F. Supp. 214 (D.Del. 1991) (discussing various readings of *Branzburg*).

[96] *New York Times*, 459 F.3d at 160.

[97] *Id.* at 173-74.

reporter's privileges.[98] *Reporters Committee* is thus a weak reed on which to stand an argument that legitimate intentions inoculate government investigations from First Amendment scrutiny.

The other thread of cases reciting the good faith investigation standard deals with undercover investigations, especially those that impinge on religious or political associations. These cases raise freedom of association conundrums because, while associational information often is relevant to criminal or counter-terrorism investigations, a fear that government agents might have infiltrated a group also is likely to chill association with and within the group. While some courts have approached the freedom of association issue head-on in these cases, others have developed a two-step approach. First, they assess compliance with the Fourth Amendment. Second, they apply two general principles: That the investigation "be conducted in good faith" and that "undercover informers adhere scrupulously to the scope of a defendant's invitation to participate in the organization."[99]

The case law taking this two-step approach is somewhat muddled because the test's connection to freedom of association scrutiny is unclear. In *United States v. Mayer*,[100] the Ninth Circuit recently discussed this problem with the "good faith investigation" standard. The court explained that, despite phrasing in earlier opinions

---

[98] Judge Wilkey's opinion in *Reporters Committee* contains a long section about the relationship between the First and Fourth amendments, which he opined that freedom of association cases, such as *NAACP v. Alabama*, "recognize only a Personal testimonial privilege to resist compelled self-disclosure. They do not apply to the good faith collection of information from Third parties." 593 F.2d at 1053-60. That part of the opinion was not joined by either of the other members of the panel, its understanding of the right to freedom of association is idiosyncratic and its conclusion that freedom of association is not implicated when information is acquired from third parties has been largely rejected by later courts, as discussed above. *Zurcher v. Stanford Daily*, another foundation for the argument that First and Fourth Amendment protections are nearly coterminous, concerned a similar issue: Whether news organizations should be subject to search warrants for evidence of third party criminal activity. It did not involve a government attempt to acquire associational information. 436 U.S. 547 (1978).

[99] United States v. Aguilar, 883 F.2d 662, 705 (9th Cir. 1989); United States v. Mayer, 503 F.3d 740 (9th Cir. 2007); Pleasant v. Lovell, *et. al.*, 876 F.2d 787 (10th Cir. 1989); Jabara v. Kelley, 476 F. Supp. 561 (E.D. Mich. 1979); Presbyterian Church v. United States, 870 F.2d 518 (9th Cir. 1989); *See also* Voss v. Bergsgaard, 774 F.2d 402, 405 (10th Cir. 1985) ([s]earch warrant authorizing seizure of documents, including "indicia of membership in or association with the NCBA" from organization engaging both in anti-tax advocacy and in potentially fraudulent transactions designed to avoid tax obligations not only lacked sufficient particularity to satisfy the fourth amendment, but was "particularly infirm given that speech and associational rights of NCBA members were necessarily implicated").

[100] 503 F.3d at 740.

suggesting that "good faith" merely means good intentions,[101] good faith demands that "an investigation threatening First Amendment rights . . . be justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests,"[102]a test that brings standard freedom of association scrutiny into the "good faith" analysis.

While there is more to be said about freedom of association's implications for undercover investigations, two points will suffice for present purposes. First, the good faith investigation approach is at best a proxy, in the undercover investigation context, for freedom of association's exacting scrutiny. It is neither a replacement for, nor a permissible end run around, for the First Amendment's requirements. Second, even in the undercover investigation context, "good faith" cannot be taken to mean simply a benevolent purpose. Benevolent intent does not ensure compliance with freedom of association's guarantees. As the Court explained in *Shelton*, "even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved."[103]

IV. THE NSA'S TELEPHONY METADATA PROGRAM AND FREEDOM OF ASSOCIATION'S SPECIFICITY REQUIREMENTS

Because of the NSA telephony metadata program's recent high profile, I use it here as a lens through which to consider the implications of freedom of association's specificity requirements for metadata surveillance.[104]

---

[101] *Aguilar*, 883 F.2d at 662.

[102] *Mayer*, 503 F.3d at 753.

[103] 364 U.S. at 488.

[104] The conceptual arguments made here do not depend very heavily on details about the NSA's metadata surveillance program. While the NSA is probably on the cutting edge, there is every reason to believe that metadata surveillance is becoming part and parcel of the law enforcement toolbox. *See* Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 1, 2013, *available at* http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html?_r=0.

A. *The Telephony Metadata Surveillance Program*

The leaks of June 2013 revealed that the NSA had been collecting "all call detail records or 'telephony metadata' created by [major carriers] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[105] This data collection was purportedly authorized under 50 USC § 1861 of FISA (commonly known as "Section 215 of the Patriot Act").[106]

Section 215 substantially expanded a pre-existing FISA business records provision to permit the FISC to issue "an order requiring the production of any tangible things (including books, records, papers, documents, and other items)"[107] upon a showing that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted [in accordance with Attorney General guidelines] . . . to protect against international terrorism or clandestine intelligence activities" provided that any such investigation of a United States person is not "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[108]

In 2006, Congress added a "minimization procedures" requirement to Section 215, restricting the dissemination of information about United States persons, and clarified that a Section 215 order "may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things."[109]

In May 2006, the FISC issued the first Section 215 order requiring telecommunications carriers to produce "comprehensive communications routing information, including but not limited to

---

[105] *See, e.g.*, In Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, No. BR 13-80 (FISA Ct. July 19, 2013).

[106] The history and interpretation of Section 215 and its use in the NSA's telephony metadata program are by now the subject of numerous analyses, including some in this symposium volume. Here I limit my discussion to points that bear on the freedom of association analysis.

[107] 18 U.S.C. § 1861 (2012).

[108] *Id.*

[109] *Id.* at (c)(2)(D).

session identifying information (e.g. originating and terminating telephone number, communications device identifier, etc.), trunk identifiers, and time and duration of call," but excluding "the substantive content of any communication . . . or the name, address, or financial information of a subscriber or customer."[110] Similar orders have been issued regularly ever since.

The FISC order mandated that the NSA access the collected metadata only "when [the] NSA has identified a known telephone number for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted name]," with the caveat that, for a phone number used by a U.S. person, the determination not be based solely on First Amendment protected activities.[111] The order included various requirements for audit and review and commanded that the data be destroyed after five years. After the NSA reported numerous instances of non-compliance with the FISC's restrictions, an audit was conducted and the program was reauthorized in 2009 with somewhat stricter provisions. In particular, querying was limited to metadata within three "hops" of a telephone number meeting the reasonable, articulable suspicion standard.[112]

Dissemination of information obtained from the metadata is subject to minimization procedures. In particular, "prior to the dissemination of any U.S. person identifying information, [one of several specified intelligence officials] must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance."[113]

Importantly, while the FISC orders[114] place important restrictions on the NSA's use of the comprehensive database, there are few

---

[110] *In Re* Application of the FBI for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 06-05 (FISA Ct. 2006) [hereinafter FISC 2006 Order].

[111] *Id.* at 5.

[112] [Redacted], No. PR/TT [Redacted] (FISA Ct. 2009) (Memorandum Opinion reinstating Telephony Metadata Program). The unredacted portion of a more recent order does not mention the "three-hop" query limitation, but refers to an "automated query process" initially approved in 2012. The Obama Administration August 2013 White Paper stated that the three-hop limitation remains in place. OBAMA ADMIN. WHITE PAPER, *supra* note 3, at 4. As discussed below, in a speech on Jan. 17, 2013. President Obama indicated that the program would be revised to limit queries to two hops. Obama's Speech, *infra* note 136.

[113] FISC 2006 Order, *supra* note 110, at 7.

[114] [Redacted], No. [Redacted] (FISA Ct. Oct. 11, 2013).

restrictions on the NSA's use of the extracted data, which is placed in a "corporate store."[115] Data in the corporate store may be queried without any requirement of reasonable articulable suspicion and need not be destroyed after five years. The FISC orders do not require an auditable record of searches of the "corporate store." The *PCLOB Report* appears to be one of the few discussions of the NSA's telephony metadata program to take note of the lack of restrictions on use of the "corporate store." The *Report* points out that, in light of the NSA's report that it used 300 seed numbers to query the primary database in 2012 and under the reasonable assumption that each telephone numbers has seventy-five contact numbers, the NSA's corporate store may house a network of upward of 120 million telephone numbers.[116] As long as there is a "valid foreign intelligence purpose," the NSA appears to be free to engage in virtually any analysis of that network.[117]

B. *The Telephony Metadata Program and Freedom of Association's Specificity Requirements*

Debate about the legality of the NSA's telephony metadata program has focused mostly on the program's compliance with Section 215 and with the Fourth Amendment. As noted earlier, two district courts recently have analyzed the Fourth Amendment question and come to opposite conclusions. The *PCLOB Report*, however, undertakes a detailed freedom of association analysis and concludes:

> The collection of telephone metadata records for all Americans' phone calls extending over a five year time period implicates the First Amendment freedom of association. Although the program is supported by a compelling government interest in combating

---

[115] There has been surprisingly little public debate about the lack of restrictions on the NSA's use of the data extracted to the "corporate store." The exception is the PCLOB Report, which discusses the issue. PCLOB REPORT, *supra* note 15, at 29-31, 164-66. The PCLOB recommends ending the Section 215 data collection and purging the corporate store. *Id.* at 169. While the program is in place, the Report recommends requiring a "reasonable articulable suspicion" determination before analysts may submit queries to, or otherwise analyze, the "corporate store," which contains the results of contact chaining queries to the full "collection store." *Id.* at 170-72.

[116] *Id.* at 30-31.

[117] *Id.* at 30, 166, 171.

> terrorism, which can justify some intrusions on First Amendment rights, it is not narrowly tailored. The extraordinary breadth of this collection program creates a chilling effect on the First Amendment rights of Americans, and we factor this concern into our policy analysis later in this Report.[118]

While I do not agree entirely with the *Report*'s analysis—which employs the less stringent election context standard of scrutiny, rather than the appropriate strict or exacting scrutiny standard[119]—the Report correctly focuses attention on freedom of association and on the specificity issue, which the courts have yet to confront.

In 2013, the FISC released two opinions considering the legality of comprehensive telephony metadata collection under Section 215.[120] In the first, the court determined that the government had met the relevance standard, interpreting relevance broadly to mean that the records have "some bearing on [] investigations of the identified international terrorist organization," and stated that the "finding of relevance most crucially depended on the conclusion that bulk collection is necessary for [the] NSA to employ tools that are likely to generate useful investigative leads," so that "the entire mass of collected metadata is relevant to investigating international terrorist

---

[118] *Id.* at 106.

[119] The Report states that "[t]he test to be applied in assessing whether the government action violates the First Amendment depends on the strength of the chilling effect" and quotes *Doe v. Reed*'s standard requiring "a substantial relation between the disclosure requirement and a sufficiently important governmental interest. To withstand this scrutiny, the strength of the governmental interest must reflect the seriousness of the actual burden on First Amendment rights." PCLOB REPORT, *supra* note 15, at 130-31, (*quoting Doe*, 130 S. Ct. at 2818). The Report cites another election case, for the proposition that "while 'severe burdens on associational rights' are subject to 'strict scrutiny,' a much lower standard of review applies when 'regulations impose lesser burdens'" and thus "[w]here the burden on the freedom of association is minimal, the state's 'important regulatory interests will usually be enough to justify reasonable, nondiscriminatory restrictions.'" PCLOB REPORT, *supra* note 15, at 132 (quoting *Clingman*, 544 U.S. at 586-87). As explained above, I contend that the strict scrutiny standard applies uniformly outside of the election context and therefore do not agree that the standard of *Doe v. Reed* and *Clingman* (which differ) are applicable here. Nonetheless, I agree with much of the Report's analysis because the Report concludes that the telephony metadata program can be expected to result in a substantial chilling effect. PCLOB REPORT, *supra* note 15, at 161-64.

[120] *In re* Application of the FBI for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 13-109 (FISA Ct. Aug. 29, 2013)[hereinafter FISC Order 13-109]; *In re* Application of the FBI for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 13-158 (FISA Ct. Oct. 11, 2013) [hereinafter FISC Order 13-158].

groups and affiliated persons."[121] The court also held that the program's constitutionality under the Fourth Amendment was "squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*," which had found no reasonable expectation of privacy in dialed telephone numbers intercepted using a "pen register."[122] In the second opinion, the court held that the Supreme Court's holding in *United States v. Jones* that location tracking using a GPS monitor constituted a search did not change the analysis.[123]

Even if the FISC's breathtakingly broad reading of "relevance" could be justified, its interpretation of Section 215 would render the provision unconstitutional on its face by permitting the equivalent of subpoenas for associational information without imposing the appropriate First Amendment standard.[124] Section 215 permits the FISC to issue an order for "tangible things" pursuant to an authorized foreign intelligence investigation as long as the investigation is "not conducted of a United States person solely upon the basis of activities protected by the First Amendment to the Constitution of the United States."[125] That standard inadequately accounts for freedom of association rights. As discussed above, a freedom of association violation need not involve illegitimate government intentions. Moreover, the standard takes no account whatsoever of the potential burden on the freedom of association rights of those who are not the targets of the investigation. It is possible to read Section 215 differently. When Congress clarified that Section 215 "may only require the production of a tangible thing if such thing can be obtained with a subpoena *duces tecum* issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things,"[126] it presumably incorporated the freedom of association scrutiny most courts apply to subpoenas and civil discovery orders. The FISC did not subject the telephony metadata program to the requisite First Amendment scrutiny. However, it did impose some restrictions on the program, as described above, which must be considered in the freedom of association analysis.

---

[121] FISC Order 13-109, *supra* note 120, at 19-20.

[122] *Id.* at 6.

[123] FISC Order 13-158, *supra* note 120, at 4-5.

[124] *See supra* Part I.A., for a discussion on freedom of association's impact on the standards for subpoenas and civil discovery orders.

[125] 50 U.S.C. § 1861(a)(2)(B)(2012).

[126] 50 U.S.C. § 1861(c)(2)(D).

The "broad and sweeping" membership disclosure requirement struck down in *Shelton* pales in comparison to the potential intrusiveness of the NSA's telephony metadata program. If the government were to demand that every telephone user in the country turn over a list of all of his or her formal and informal associations based on a general assertion that the lists would be "relevant to investigating international terrorist groups and affiliated persons," there is no chance that the inquiry would pass muster under freedom of association doctrine. Such a sweeping demand for associational information would chill association for the reasons articulated in *Shelton*. Though the interest in identifying terrorist operatives or networks is compelling, such a mandate would fail the specificity requirement on numerous grounds, including: The lack of specificity of the compelling government interest in terrorism; the lack of a tight fit between the vast majority of associations and the identification of terrorists; the unfettered discretion afforded to government officials who had access to the lists; and the availability of more focused investigations of particular groups based on specific reasons to believe that they or their members are involved in terrorist activity.

The NSA's telephony metadata program differs from such a plainly unconstitutional inquiry in several respects, which might be argued to bring it within the constitutional strictures. First, the metadata must be analyzed, rather than merely perused, to obtain meaningful information about associations. Second, the FISC's order permits the NSA to query the comprehensive database only if NSA officials have determined that the query seed meets the reasonable articulable suspicion standard and only out to three "hops." Proposals to cabin the program have been aimed primarily at beefing up these limitations by reducing the number of "hops" to two and subjecting the reasonable articulable suspicion determination to judicial oversight, either prospectively or by regular audit. Third, the NSA may not share "U.S. person information" outside the agency unless an appropriate official determines that it "is in fact related to counterterrorism information" and "is necessary to understand the counterterrorism information or assess its importance."[127]

In and of itself, the fact that associational information must be inferred from the metadata rather than merely read from a list does little to limit the program's potential to chill associational activity and lack of specificity. There is no question that the telephony metadata can be used to infer associational information. Indeed, the NSA justifies collecting it on the grounds that it will be useful for inferring membership in terrorist networks and undoubtedly is developing and

---

[127] FISC Order 13-109, *supra* note 120, at 13; *see also* PCLOB REPORT, *supra* note 15, at 32.

using social network analysis tools for that purpose.[128] The government cannot be permitted to exploit the intertwined social and technological changes that have made it possible to use metadata to avoid direct demands for associational information to circumvent basic freedom of association guarantees.[129] Like the associational information demanded in *Shelton*, the trove of telephony metadata could in principle allow government officials to explore "every conceivable kind of associational tie—social, professional, political, avocational, or religious."[130] Government access to associational data for virtually all citizens creates a potential for abuse of discretion even greater than that created by the state's collection of associational information from teachers in *Shelton* and is likely to result in even more profound chilling effects.

Counterterrorism is, of course, a compelling government interest. However, a comprehensive pool of telephony metadata bears no specific relationship to that interest. Section 215 authorizes acquisition of data pursuant to an authorized investigation. Indeed, the FISC's orders appear to name particular organizations (the names are redacted), which presumably are the targets of authorized counter-terrorism investigations. Nonetheless, there is no specific connection between the amassing of comprehensive telephony metadata and any particular investigatory target. The government essentially admits as much when it argues that its queries have involved only a small fraction of the data it has collected.

The government has argued that "the program's objectives could not be achieved . . . [through targeted collection of] metadata associated only with the calls of persons already known to be, or suspected of being, terrorist operatives." That is not the proper question. The proper question is whether the comprehensive collection of telephony metadata advances the compelling interest of "identifying terrorist operatives and preventing terrorist attacks" sufficiently more effectively than less intrusive alternatives, such as staged acquisition of call data for individuals about whom a requisite level of suspicion is reached.[131] The FISC's conclusion that "bulk

---

[128] It is true that the metadata does not contain "names and addresses" corresponding to telephone numbers. Matching telephone numbers to names is usually a trivial matter using publicly available resources. In any event, one assumes that the NSA has that capability or the data would not be of much use for its own purposes.

[129] *See* discussion, *supra* Part I.A.

[130] *See* 364 U.S. at 488.

[131] *See, e.g.*, Strandburg, *supra* note 2; USA FREEDOM Act, H.R. 3361 and S. 1599, § 101 (proposal to amend Section 215 to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought—(i) are relevant and material

collection is necessary for [the] NSA to employ tools that are likely to generate useful investigative leads" similarly begs the important question, which is whether those "tools" are necessary to advance the government's interests.

The available evidence suggests that the telephony metadata program advances the government's counterterrorism interests only marginally, if at all, and that the same results could have been obtained by focused requests for particular call records using other legal authorities.[132] The government's argument reduces in the end to the contention that there might be some circumstance under which the time saved by having the data on hand was critical in averting a terrorist incident.[133] That argument proves too much. Undoubtedly, one could argue that government acquisition of complete historical records of every individual's associations would be useful for law enforcement and counterterrorism efforts, as would complete records of their locations, their transactions and their conversations. The convenience of total surveillance is not a sufficient justification. In fact, there undoubtedly are many other, more focused, steps, including some entirely unrelated to telephony metadata, that the government could take to advance the general interest in counterterrorism with significantly less imposition on freedom of association interests.

Of course, the FISC orders impose limitations on the NSA's use of the data collection. The question is whether those limitations overcome the freedom of association failings just described. The restrictions imposed by the FISC orders have several weaknesses in this regard. They do relatively little to cabin the government's discretion, and hence little to reduce the chilling effect of the data collection. Critical determinations, such as whether there is reasonable articulable suspicion and whether a U.S. person's identity is "related to counterterrorism information" and "necessary to understand the counterterrorism information or assess its

---

to an authorized [foreign intelligence] investigation . . . and (ii) pertain to—(I) a foreign power or an agent of a foreign power; (II) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (III) an individual in contact with, or known to, a suspected agent of a foreign power; . . .).

[132] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 13; PCLOB REPORT, *supra* note 15.

[133] OBAMA ADMIN. WHITE PAPER, *supra* note 3. The government also argues that its comprehensive collection of telephony metadata is necessary because telephone companies might not retain their data for sufficiently long periods of time. *Id.* An obvious alternative would be to impose data retention requirements on carriers. Without taking a position on whether such requirements would be a good idea as either a legal or political matter, one can easily conclude that they would be less burdensome than government collection.

importance"[134] are made entirely within the executive branch and are not subject to judicial review. There is thus no opportunity for a court to assess, for example, whether the reasonable articulable suspicion standard, as applied by the NSA, is sufficiently stringent to justify the sweeping inquiry into the target individual's associations permitted by a three-hop query.[135] Even more importantly, the FISC order takes no account whatsoever of the freedom of association burdens imposed by the NSA's virtually complete discretion with respect to its analysis of the data (most of which relates to associations about which there is no whiff of terrorism) that has been transferred to the "corporate store."

Particularly for those who share religious, ethnic, or political identities with groups that are under investigation, an unreviewed reasonable articulable suspicion standard and a three hop limitation are likely to do little to reduce the fear that engaging in expressive activities will raise suspicion about them or bring them into indirect contact with those the government already has deemed suspicious, thus embroiling them in counter-terrorism investigations. In light of the marginal effectiveness of the program, it seems unlikely that these limitations sufficiently reduce the freedom of association burden.

In a speech on January 17, 2014, President Obama laid out changes that he intended to make to the Section 215 program.[136] First, he stated that "effective immediately," the NSA would "only pursue phone calls that are two steps removed from a number associated terrorist organization."[137] He also indicated that the attorney general would work with the FISC so that "the database can be queried only after a judicial finding or in the case of a true emergency."[138] He also stated that it would begin a process of developing options to "match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this metadata itself."[139]

---

[134] FISC Order 13-158, *supra* note 120.

[135] The standard might be compared, for example, to the standard for determining whether an organization is a "communist-action organization" from which membership information could be demanded. See discussion, *supra* Part II.C.

[136] *Obama's Speech on N.S.A. Phone Surveillance*, N.Y. TIMES, Jan. 17, 2014, *available at* http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html.

[137] *Id.* at 11.

[138] *Id.*

[139] *Id.*

The President's Review Group recommended that the government's bulk collection of telephony metadata be terminated and transitioned to "a system in which such meta-data is held instead either by private providers or by a private third party."[140] It further recommended that queries of the data should comply with an amended Section 215 standard requiring not only that the information be relevant to an authorized counterterrorism investigation, but also that "like a subpoena, the order is reasonable in focus, scope, and breadth."[141]

The PCLOB recommended the termination of the bulk telephony metadata program and the immediate purging of the data in the primary database and the corporate store. Failing that (or in the meantime), the PCLOB recommended that the government:

> (a) Reduce the retention period for the bulk telephone records program from five years to three years;
>
> (b) Reduce the number of "hops" used in contact chaining from three to two;
>
> (c) Submit the NSA's "reasonable articulable suspicion" determinations to the FISC for review after they have been approved by NSA and used to query the database; and
>
> (d) Require a "reasonable articulable suspicion" determination before analysts may submit queries to, or otherwise analyze, the "corporate store," which contains the results of contact chaining queries to the full "collection store."[142]

Each of these suggestions would likely reduce the chilling effect of the telephony metadata program to some degree, primarily by reducing the government's discretion in analyzing the data. Only the PCLOB's recommendations deal with the corporate store's "ever-growing subset of telephone calling records."[143] That is a serious

---

[140] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 13, at 25.

[141] *Id.* at 24.

[142] PCLOB REPORT, *supra* note 15, at 170.

[143] *Id.* at 171.

omission and I am highly doubtful that the telephony metadata program can be adequately tailored to meet freedom of association scrutiny without restricting the use of the data contained in the corporate store. Long-term storage in the corporate store increases the potential for chilling effects and abuse significantly, while it is entirely unclear what it adds to the already dubious benefits of the telephony metadata program.

I am not sure, however, that the PCLOB's proposed reasonable articulable suspicion standard is the answer.[144] For one thing, it is not entirely clear what the proposed standard means, given that there are no limitations on the types of analyses that can be performed on data in the corporate store. Since every number in the corporate store is within three hops (now two) of a number for which there was reasonable articulable suspicion, it would seem that nearly any analysis one would want to do on a number for which there is no reasonable articulable suspicion could be framed as an analysis that begins on the applicable seed, hops to that number and proceeds from there. Another effect of long-term storage in the corporate store is that it permits the NSA to retain and continue to analyze data derived from seeds to which reasonable articulable suspicion no longer applies. Perhaps the proposed standard is intended to take such data off the table. Long-term storage in the corporate store also avoids the limit on data retention in the primary database, but the proposed standard would not appear to change that.

In the end, the bulk telephony metadata program, even if it is made more specific by the proposed changes, seems likely to fail freedom of association scrutiny because of its marginal efficacy in light of the substantial chilling effects it is likely to continue to engender. It thus continues to seem likely that alternative steps could be taken with comparable counterterrorism impact and substantially less burden on freedom of association. For example, as I suggested in my 2008 article, a staged approach in which at each hop metadata is collected only for those individuals about whom there is a requisite level of suspicion (which might be provided by further investigation) might provide comparable benefit. If such an approach were employed simultaneously on a group of numbers meeting the reasonable articulable suspicion standard, for example, it would uncover any unknown numbers that were in contact with more than one reasonable articulable suspicion-approved seed. Those numbers could then be investigated to determine whether to include them in

---

[144] Of course, neither are the PCLOB Report's authors, who advocate termination of the program in its entirety. *Id.* at 168.

the reasonable articulable suspicion-approved network. The marginal benefits of adding two-hop data may not be significant.

V. CONCLUSION

The primary message of this article is that freedom of association scrutiny applies to government acquisition of "metadata" and subjects it to specificity requirements. Those requirements are unlikely to be satisfied by sweeping data collection programs, such as the NSA's telephony metadata program, that are not specifically targeted to make a significant impact on a specific compelling government interest. Though recent proposals to limit the program go some way toward reducing its likely chilling effects, they are unlikely to compensate for the program's marginal efficacy, meaning that there are likely to be substantially less burdensome means to make similar progress toward counterterrorism goals.